

Fault Management Scope in Theory and in Practice

Dr. Stephen B. Johnson

sjohns22@uccs.edu and stephen.b.johnson@nasa.gov

*NASA MSFC EV43 Integrated System Health Management and Automation Branch
&
University of Colorado at Colorado Springs - Jacobs ESTS*

12 April 2012

Fault Management in Theory



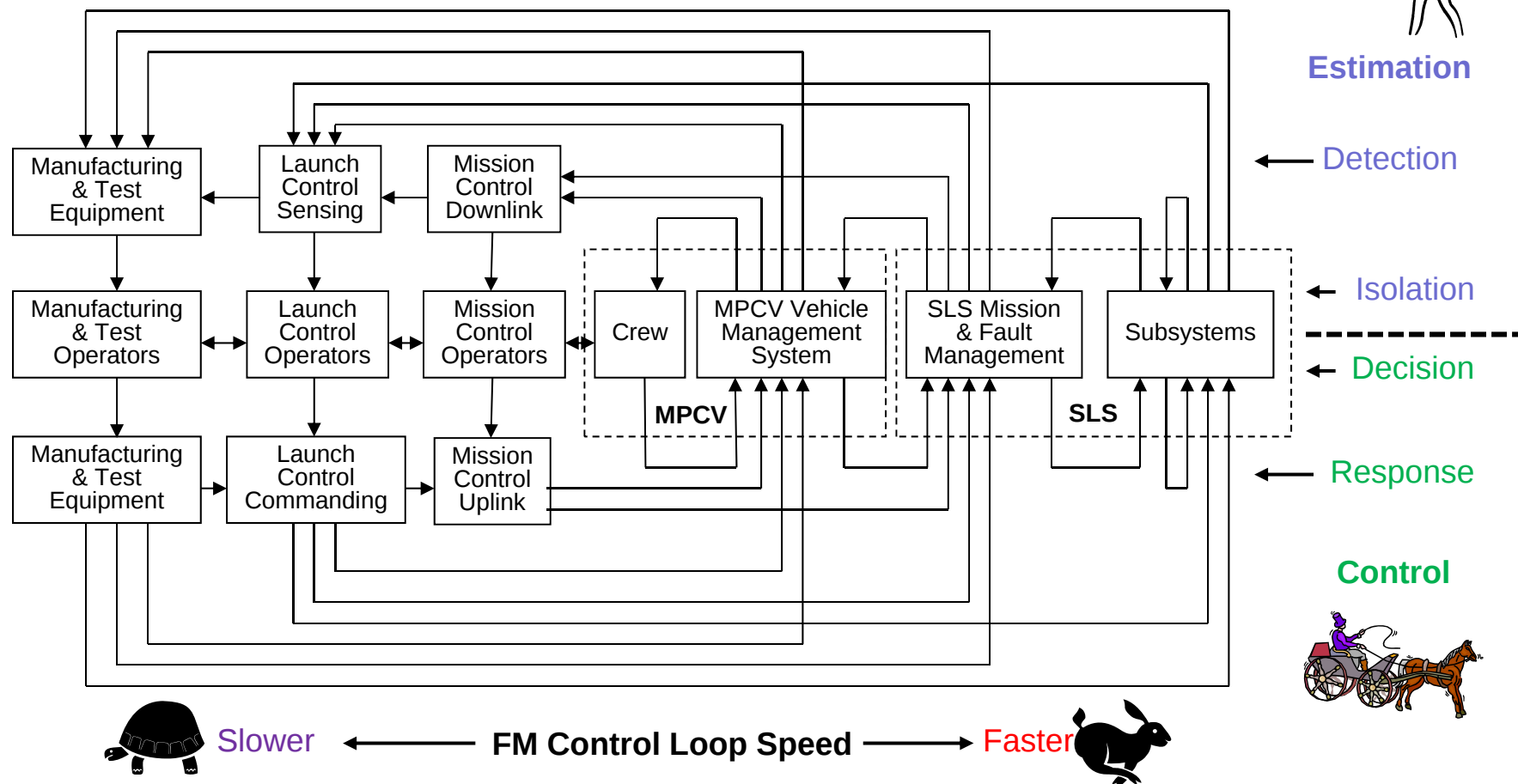
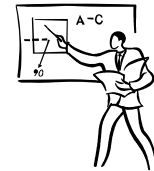
- ◆ **The operational subset of System Health Management**
- ◆ **A set of “meta-control loops” that aim to restore the system to a state that is controllable by nominal (passive and/or active) control systems**
 - Usually the regular (passive or active) control system has been compromised because (for active control) its sensors, processing, or actuators are compromised, or (for passive control) the design margins have eroded to zero or negative
- ◆ **Each loop consists of failure detection, isolation, decision, and response**
 - Variants include different detection types (anomalies or degradations), prognostics, failure identification, and different response types (recovery, goal change, operational fault avoidance)
- ◆ **The newly-controllable state might or might not be to the system’s original goals**
 - If original goals sustained, then we have failure recovery
 - Example: computer voting, redundancy management
 - If original goals not sustained, then we have a goal change, usually to some subset or degraded version of the original system goals
 - Example: vehicle safing or crew abort
- ◆ **Control theory applies: state estimation and control = failure detection/isolation and failure response decision/execution**
- ◆ **Systems theory applies: system boundaries and recursion**

Generic Launcher and Crew Fault Management Architecture



FM Conceived as a set of control loops in the system architecture, each entire loop from detection through response/recovery must be addressed to determine effectiveness

Total effectiveness = probabilistic summed effectiveness of all loops to improve reliability, availability, safety (RAS)

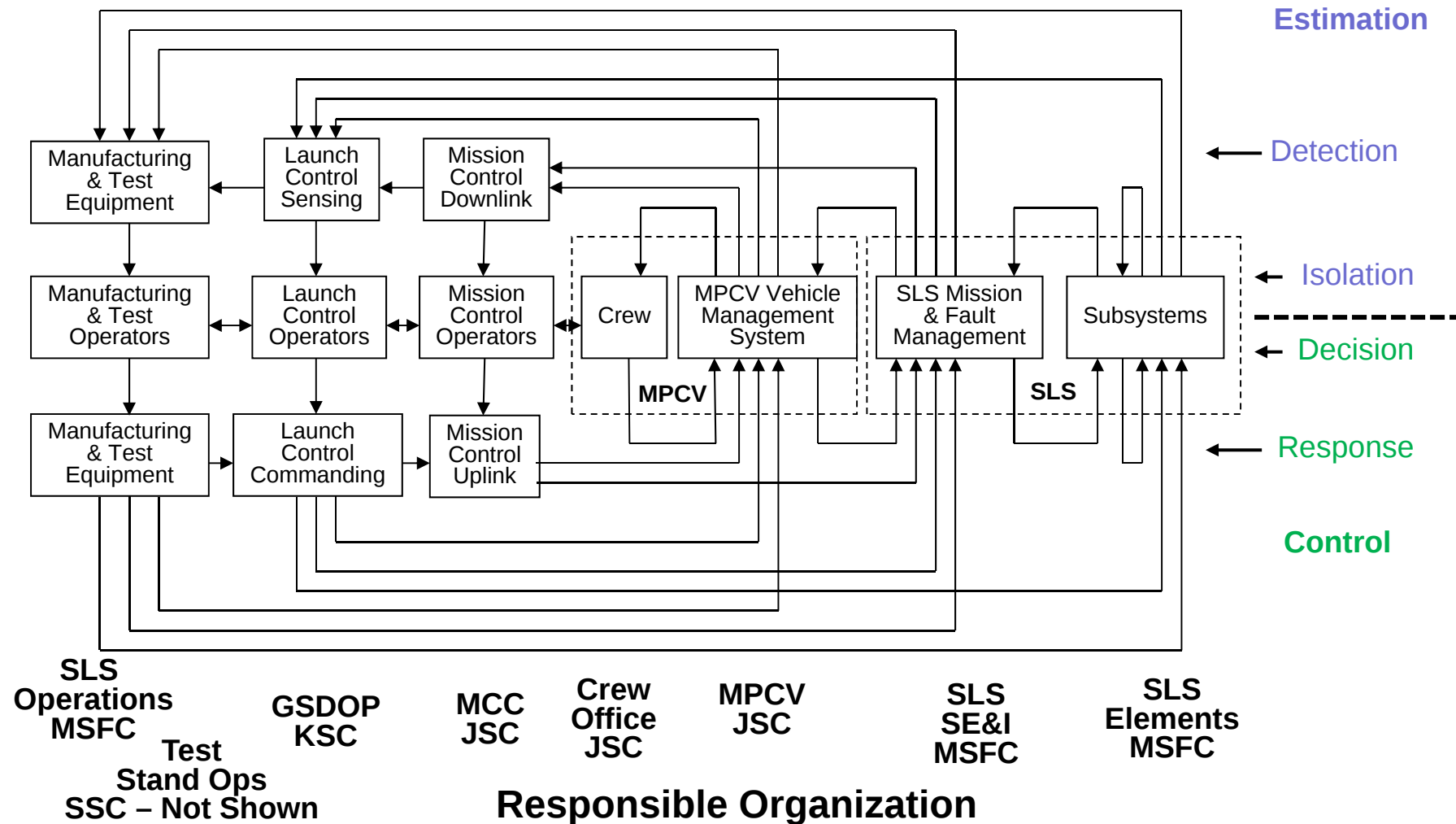


The FM Organizational Implementation Issue



Who is responsible for the entire FM design and analysis?

NASA's system distributes responsibility, which can create gaps / holes in FM/SHM design and analysis.



Analysis Organizational Issue



- ◆ **For large programs and human spaceflight, S&MA is responsible for reliability, availability, safety, hazard analyses and FMEAs**
- ◆ **Operations organizations responsible for pre-launch, and in-flight activities**
 - Contingency planning, trending, anomaly resolution, repair/maintenance, etc.
- ◆ **How do FM analysts interact with S&MA and operations?**
- ◆ **Each project must assess, but in general, there must be some means to integrate all of the calculations and analyses for RAS**
- ◆ **S&MA the logical place to integrate the calculations at the highest levels for the entire system**
- ◆ **FM responsible for the effectiveness calculations of the FM design, whether implemented by engineering or operations**
 - Necessary to determine if the FM design is effective to meet FM requirements



Why This Matters

◆ Example from Magellan --- 1989

- First triggering of Fault Protection (FP), on-board FP works fine to detect a problem with star scanner and safe the system (point to Earth)
- Mission operations recovery fails, and re-triggers on-board FP again
- Designers had written operations rule to prevent the operations recovery mistake, but if you don't know there's a potential issue, you don't look for it!

◆ Current SLS Example

- Abort design and analysis requires contributions from many organizations, extraordinarily complex, both technically and organizationally

◆ Institutional separation creates interfaces

◆ FM / SHM often not recognized in NASA procedures, and even where it is recognized, the institutional implementation usually remains divided

◆ Who is responsible for the entire design, when the FM Control Loop implementation crosses organizational boundaries??

- When nobody is responsible, risks of failure increase significantly
- The problem exists within projects, not only across projects... local subsystem FM versus global system FM

◆ Critical to establish clear organizational relationships of FM design, analysis, testing with others in engineering, ops, and S&MA